Iterations of Linear Maps over Finite Fields

Michał Misiurewicz

Department of Mathematical Sciences, Indiana University Purdue University Indianapolis, Indianapolis, IN 46202-3216

John G. Stevens

Department of Mathematical Sciences, Montclair State University, Upper Montclair, NJ 07043

Diana M. Thomas

Department of Mathematical Sciences, Montclair State University, Upper Montclair, NJ 07043

Abstract

We study the dynamics of the evolution of Ducci sequences and the Martin-Odlyzko-Wolfram cellular automaton by iterating their respective linear maps on $\mathbb{Z}_2^n$. After a review of an algebraic characterization of cycle lengths, we deduce the relationship between the maximal cycle lengths of these two maps from a simple connection between them. For n odd, we establish a conjugacy relationship that provides a more direct identification of their dynamics. We give an alternate, geometric proof of the maximal cycle length relationship, based on this conjugacy and a symmetry property. We show that the cyclic dynamics of both maps in dimension $2n$ can be deduced from their periodic behavior in dimension n. This link is generalized to a larger class of maps. With restrictions shared by both maps, we obtain a formula for the number of vectors in dimension $2n$ belonging to a cycle of length q that expresses this number in terms of the analogous values in dimension n.

Key words: Ducci sequences, cellular automata, dynamics of linear maps
2000 MSC: Primary 11T06, 15A33; Secondary 37B15, 39A10

Email addresses: mmisiure@math.iupui.edu (Michał Misiurewicz), stevensj@mail.montclair.edu (John G. Stevens), thomasdia@mail.montclair.edu (Diana M. Thomas).

[1] The first author was supported in part by NSF Grant DMS 0139916

1 Introduction

Iterations of linear maps on finite dimensional vector spaces over finite fields appear in different areas of mathematics ranging from number theory to mathematical physics. We begin our discussion with a number theoretic example.

Dynamics of the linear map given by

$$D_n\mathbf{x} = (x_1 + x_2, \ldots, x_n + x_1), \tag{1}$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, was initially studied by E. Ducci in the case when n is a power of 2 in the late 1800's. Because $\mathbb{Z}_2^n$ is a finite set, the sequence of images, $D_n^k(\mathbf{x})$, $k = 1, 2, 3, \ldots$ will be eventually periodic. That is, there will be two nonnegative integers, $l \neq m$ such that $D_n^l(\mathbf{x}) = D_n^m(\mathbf{x})$. The number of distinct vectors that appear in the cycle (that is, the period of this cycle) will be called the *cycle length*. Since its original posing, the problem of finding cycle lengths of the map as a function of arbitrary n appears extensively in the number theory literature, [1,6,12].

Dynamics of the Ducci map was considered in the finite field setting by Calkin, Stevens and Thomas in [2] who obtained characterizations of cycle lengths for D_n. Note D_n is linear.

Many applications also appear naturally as cellular automata. A finite dimensional cellular automaton (CA) is a discrete time dynamical system usually defined on the vector space $\mathbb{Z}_2^n$. Each component of a vector in $\mathbb{Z}_2^n$ is thought of as a "cell" whose state is updated by a local deterministic rule.

An example of a finite dimensional CA is the Martin-Odlyzko-Wolfram (MOW) map [13]. In this paper when we work with vectors such as $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$ then the addition and subtraction of the indices will be performed modulo n. Thus, $n + 1$ should be understood as 1, $1 - 1$ as n, etc. With this notation, the MOW map updates an initial vector

$$(x_1(0), x_2(0), \ldots, x_n(0)) \in \mathbb{Z}_2^n,$$

through the rule

$$x_i(1) = x_{i-1}(0) + x_{i+1}(0).$$

The local rule acting on a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$ can be aggregated as the single linear map defined by

$$M_n\mathbf{x} = (x_n + x_2, x_1 + x_3, \ldots, x_{n-1} + x_1). \tag{2}$$

As a result, the dynamics of this rule can be understood using finite field theory and linear algebra.

The concept of CA as a dynamical system on a vector space over a finite field was employed by Martin, Odlyzko and Wolfram in their 1984 paper [13]. Since 1984, many articles have appeared extending and generalizing the results in [13] to other linear rules [9,10,16,17,19].

E. Jen characterized limit cycle structure through orders of minimal polynomials for CA defined on a cylinder [9,10]. Stevens extended this result by proving that all cycle lengths under iteration by any linear transformation can be obtained as orders of minimal annihilating polynomials [17] (see also [14]). Moreover, the transient behavior can be obtained from the number of factors of λ contained in the minimal polynomial.

The purpose of this paper is twofold. Although interest in the iterative behavior of D_n and M_n originated from two separate areas of mathematics, the maps share several surprising properties. The first goal of this paper is to state these specific relationships. Motivated by parallel characteristics of both maps, our second goal is to generalize the results.

Section 2 of this paper introduces the language used in [2,18] to analyze linear maps over a finite field through minimal polynomials. In Section 3, the history and mathematical background of D_n and M_n are provided. Specific relationships between D_n and M_n such as cycle lengths of one map written as a function of cycle lengths of the other are obtained in Section 4. It is found that one can lift the dynamics of both D_n and M_n from dimension n to $2n$. Section 5 generalizes this property to a large class of maps and then uses the result to answer specific questions about the dynamics of D_n and M_n.

2 Characterization of cycle lengths as orders of minimal annihilating polynomials

This section provides an overview of how to characterize cycle length and transient behavior of a linear map defined on a vector space over a finite field through orders of minimal annihilating polynomials. The purpose of such a characterization is to provide an alternative to iterating every possible vector in order to understand the global dynamics of a map. In addition, because algorithms for computing orders of polynomials are included in computer algebra software such as Maple, it is possible to compute all possible cycle lengths generated by the map in a reasonable amount of time.

The present discussion is posed over $\mathbb{Z}_2$ due to the applications considered in this paper. However, all the statements in this section hold over any finite field of characteristic p. The next few definitions are standard and appear in [8].

Definition 2.1 *Let A be an $n \times n$ matrix with entries from $\mathbb{Z}_2$. The minimal annihilating polynomial of a vector $\mathbf{v} \in \mathbb{Z}_2^n$ is the monic polynomial $\mu_v(\lambda)$ of least degree such that $\mu_v(A)\mathbf{v} = 0$.*

The existence of a minimal annihilating polynomial is guaranteed by the Cayley-Hamilton theorem which states that the characteristic polynomial of A will annihilate the matrix itself. We now define the order of a polynomial [8].

Definition 2.2 *Suppose that $\mu_v(0) \neq 0$. Then the order of $\mu_v(\lambda)$, $\mathrm{ord}(\mu_v(\lambda))$, is defined to be the smallest natural number, c, such that $\mu_v(\lambda)|\lambda^c - 1$. If $\mu_v(0) = 0$, then $\mu_v(\lambda)$ can be written as $\lambda^k\tilde{\mu_v}(\lambda)$ for some positive integer k, where $\tilde{\mu_v}(0) \neq 0$. In this case, the order of $\mu_v(\lambda)$ is defined to be the order of $\tilde{\mu_v}(\lambda)$.*

In the future, we will identify the matrix A with the linear map that it defines (we use the standard basis).

For any $n \times n$ matrix A acting on $\mathbb{Z}_2^n$, the cycle length of a vector under forward iteration of A is equal to the order of its minimal annihilating polynomial. Furthermore, the number of forward iterates of the map not in a cycle can be found by factoring the minimal annihilating polynomial. The proof of the statement that follows can be found in [18].

Theorem 2.3 *Let $\mathbf{v} \in \mathbb{Z}_2^n$. Let $\mu_v(\lambda)$ be the minimal annihilating polynomial of $\mathbf{v}$. Assume that $\mu_v(\lambda) = \lambda^k\tilde{\mu_v}(\lambda)$ where $k \geq 0$ and $\tilde{\mu_v}(\lambda)$ is a monic polynomial with $\tilde{\mu_v}(0) \neq 0$. Then $A^k(\mathbf{v})$ belongs to a cycle with cycle length $c = \mathrm{ord}(\mu_v)$.*

It is well known that minimal annihilating polynomials are factors of the minimal polynomial [8]. Therefore, all possible cycle lengths can be obtained from the minimal polynomial of A. Moreover, the maximal cycle length is equal to the order of the minimal polynomial because there exists at least one vector whose minimal annihilating polynomial is equal to the minimal polynomial [8].

It is important from a dynamical systems perspective to connect the images of a vector $\mathbf{v}$ under iterates of A to the minimal annihilating polynomial of $\mathbf{v}$. If $\mathbf{v} \in \mathbb{Z}_2^n$ is a vector contained in a cycle under A, then the *algebraic period* of $\mathbf{v}$ under A is the minimal positive integer value a such that $A^a\mathbf{v}$ is a linear combination of $\mathbf{v}, A\mathbf{v}, A^2\mathbf{v}, \ldots A^{a-1}\mathbf{v}$. If a is the algebraic period of $\mathbf{v}$ then we may write

$$A^a\mathbf{v} = b_1\mathbf{v} + b_2A\mathbf{v} + \ldots b_{a-1}A^{a-1}\mathbf{v}.$$

Then the minimal annihilating polynomial of A is given by

$$\lambda^a - b_{a-1}\lambda^{a-1} - \ldots - b_2\lambda - b_1.$$

Thus, a equals the degree of $\mu_v(\lambda)$. The concept of an algebraic period was discussed in [11] although not named as such.

3 Ducci map and MOW map

This section addresses D_n and M_n using the language of minimal polynomials.

3.1 Ducci map

As stated in the introduction, E. Ducci posed the initial questions surrounding the Ducci map in the late 1800's. In its original form, the Ducci map was defined on the ring module $\mathbb{Z}^n$

$$\tilde{D}_n(\mathbf{x}) = (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_n - x_1|) \tag{3}$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ [7]. Misiurewicz and Schinzel observed that every initial n string in $\mathbb{Z}^n$ under forward iteration of $\tilde{D}_n$ converges in a finite time to a periodic solution of the form $k(x_1, x_2, \ldots, x_n)$ where $x_i \in \{0, 1\}$ and k is a positive constant [15].

The map (3) restricted to the invariant vector space $\mathbb{Z}_2^n$ is the linear map (1) which also appears as Wolfram's Rule 102 in [20]. The matrix representation of D_n in the standard basis, $\mathbf{e}_i = (0, \ldots, 1, \ldots 0)$, where the 1 appears in the i^{th} component, is

$$A_{D,n} = \begin{pmatrix} 1 & 1 & 0 & \ldots & & 0 \\ 0 & 1 & 1 & 0 & \ldots & 0 \\ & & & \ddots & & \\ 0 & & \ldots & 0 & 1 & 1 \\ 1 & 0 & & \ldots & 0 & 1 \end{pmatrix}. \tag{4}$$

The problems of interest regarding the dynamics of D_n are:

(1) Characterize cycle lengths for arbitrary n without computing the orbit of every possible vector in $\mathbb{Z}_2^n$.
(2) Find a closed form expression for the cycle lengths as a function of n.
(3) Characterize the complexity of the map by calculating the number of different cycle lengths as a function of n.

Since $A_{D,n}$ is a matrix, Question 1 can be answered using Theorem 2.3. We

illustrate how to apply Theorem 2.3 to obtain cycle lengths and transient dynamics for $n = 17$.

Example The minimal polynomial of $A_{D,n}$ computed in [2] is

$$\mu_{A_{D,n}}(\lambda) = (1+\lambda)^n + 1. \tag{5}$$

For $n = 17$

$$\mu_{D,n} = \lambda(\tilde{\mu}(\lambda)) = \lambda g_1(\lambda) g_2(\lambda),$$

where

$$g_1(\lambda) = \lambda^8 + \lambda^7 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda^2 + 1$$

and

$$g_2(\lambda) = \lambda^8 + \lambda^5 + \lambda^3 + \lambda^2 + 1$$

(cf. [14]).

The order of g_1 is 85 and the order of g_2 is 255. Although the majority of cycles are of length 255, there do exist three cycles of length 85.

Moreover, because $k = 1$ in reference to Theorem 2.3, we know that the *first* image of any vector will belong to a cycle.

An algorithm to obtain the cycle lengths for a linear map on $\mathbb{Z}_p^n$ based on minimal annihilating polynomials appears in [17]. Application of the algorithm to both the Ducci map and the MOW map for dimensions $3 \leq n \leq 40$ are provided in Table 1.

Although Question 2 is still open, Ehrlich was able to prove divisibility conditions for maximal periods for odd n [5]. Specifically, he showed for n odd,

(1) The period of the maximal cycle, $c_{D,n}$, divides c_1 where $c_1 = 2^j - 1$ and j is the smallest positive integer such that $n|(2^j - 1)$.
(2) If $n|2^l + 1$, for some l, then let $m = \min\{l : n|(2^l + 1)\}$ and define $c_2 = n(2^m - 1)$. In this case $c_{D,n}$ divides c_2.

Divisibility conditions were not obtained for even n. However, a simple application of the minimal polynomial characterization shows that any cycle length in even dimension $n = 2^j r$ where r is odd is equal to a power of two times the cycle length in dimension r. This observation is stated formally in the following theorem.

Theorem 3.1 *Let $n = 2^m r$ where $m \geq 1$ and $r \geq 1$ is odd. Let $c_{D,n}$ be the order of the minimal polynomial for $A_{D,n}$. Then $c_{D,n} = 2^m c_{D_r}$ where c_{D_r} is the order of the minimal polynomial of $A_{D,r}$.*

Vector Length	**Cycle Lengths** D_n	**Cycle Lengths** M_n	**Vector Length**	**Cycle Lengths** D_n	**Cycle Lengths** M_n
$n = 3$	$1, 3$	1	$n = 22$	$1, 341, 682$	$1, 31, 62$
$n = 4$	1	1	$n = 23$	$1, 2047$	$1, 2047$
$n = 5$	$1, 15$	$1, 3$	$n = 24$	$1, 3, 6, 12, 24$	$1, 2, 4, 8$
$n = 6$	$1, 3, 6$	$1, 2$	$n = 25$	$1, 15, 25575$	$1, 13, 1023$
$n = 7$	$1, 7$	$1, 7$	$n = 26$	$1, 819, 1638$	$1, 63, 126$
$n = 8$	1	1	$n = 27$	$1, 3, 63, 13797$	$1, 7, 511$
$n = 9$	$1, 3, 63$	$1, 7$	$n = 28$	$1, 7, 14, 28$	$1, 7, 14, 28$
$n = 10$	$1, 15, 30$	$1, 3, 6$	$n = 29$	$1, 475107$	$1, 16383$
$n = 11$	$1, 341$	$1, 31$	$n = 30$	$1, 3, 5, 6, 10, 15, 30$	$1, 2, 3, 6, 15, 30$
$n = 12$	$1, 3, 6, 12$	$1, 2, 4$	$n = 31$	$1, 31$	$1, 31$
$n = 13$	$1, 819$	$1, 63$	$n = 32$	1	1
$n = 14$	$1, 7, 14$	$1, 7, 14$	$n = 33$	$1, 3, 341, 1023$	$1, 31$
$n = 15$	$1, 3, 5, 15$	$1, 3, 15$	$n = 34$	$1, 85, 170, 255, 510$	$1, 5, 10, 15, 30$
$n = 16$	1	1	$n = 35$	$1, 7, 15, 105, 819, 4095$	$1, 3, 7, 21, 4095$
$n = 17$	$1, 85, 255$	$1, 5, 15$	$n = 36$	$1, 3, 6, 12, 63, 126, 252$	$1, 2, 4, 7, 14, 28$
$n = 18$	$1, 3, 6, 63, 126$	$1, 2, 7, 14$	$n = 37$	$1, 3233097$	$1, 87381$
$n = 19$	$1, 9709$	$1, 511$	$n = 38$	$1, 9709, 19418$	$1, 511, 1022$
$n = 20$	$1, 15, 30, 60$	$1, 3, 6, 12$	$n = 39$	$1, 3, 455, 819, 1365, 4095$	$1, 63, 1365, 4095$
$n = 21$	$1, 3, 7, 21, 63$	$1, 7, 63$	$n = 40$	$1, 15, 30, 60, 120$	$1, 3, 6, 12, 24$

Table 1
Cycle lengths under iterations of D_n and M_n.

Proof It was shown in [2] that the minimal polynomial of $A_{D,n}$ is given by

$$\mu_{A_{D,n}}(\lambda) = (1 + \lambda)^n + 1.$$

Substituting $n = 2^m r$ and expanding modulo 2 yields

$$\mu_{A_{D,n}}(\lambda) = (1 + \lambda)^{2^m r} + 1 = \left((1 + \lambda)^r + 1\right)^{2^m} = \left(\mu_{D,r}(\lambda)\right)^{2^m}.$$

A result in [11] implies that if c_{D_r} is the order of the $\mu_{D,r}(\lambda)$, then $2^m c_{D_r}$ is the order of $\left(\mu_{D,r}(\lambda)\right)^{2^m}$. $\square$

Corollary 3.2 *Let $s_{D,n}$ be a cycle length of D_n. Then $s_{D,n} = 2^i s_{D_r}$, $1 \leq i \leq m$, where s_{D_r} is a cycle length for D_r.*

Proof The corollary holds since the minimal annihilating polynomials are products of factors of the minimal polynomial. Let μ_{v_r} be a minimal annihilating polynomial for $A_{D,r}$ applied to $\mathbf{v}$. Then $\mu_{v_r}^{2^i}, 0 \leq i \leq m$ will be one of the factors of the minimal polynomial. Thus, the order of $\mu_{v_r}^{2^i}$ will be a cycle length for D_n. $\square$

Writing cycle lengths in dimension $2n$ as a function of cycle lengths in dimension n will be generalized in Section 5. Question (3) still remains unanswered and appears as an open question in [4].

3.2 MOW map

The MOW map, defined by (2) was first studied in the finite field setting by Martin, Odlyzko and Wolfram in [13]. The map is listed as Wolfram's Rule 90 in [20]. As in the case of D_n, the minimal polynomial characterization of cycle lengths requires the matrix representation of M_n in the standard basis

$$A_{M,n} = \begin{pmatrix} 0 & 1 & 0 & \dots & & 0 & 1 \\ 1 & 0 & 1 & 0 & \dots & & 0 \\ & & & \ddots & & & \\ 0 & & & \dots & 1 & 0 & 1 \\ 1 & 0 & \dots & & 0 & 1 & 0 \end{pmatrix} \tag{6}$$

Computations of the characteristic and minimal polynomials of Wolfram's Rule 90 are more technical than those for $A_{D,n}$ and appear in [18]. The calculations rely on a dimensional analysis and the algebraic period of vectors.

Although the closed form expression for the minimal polynomial of $A_{M,n}$ is not elegant, it can be used to show that $\mu_{M,n}(\lambda) = \lambda\tilde{\mu}(\lambda)$ for odd n where $\tilde{\mu}(0) \neq 0$. This is a property shared by the minimal polynomial of $A_{D,n}$. Thus, by Theorem 2.3, for odd n, the image of any vector under either map must belong to a cycle.

4 Connection between D_n and M_n.

Although interest in the map M_n originated as a CA and the focus on D_n was number theoretic, the two maps are connected through the equality

$$M_n = S_n D_n^2, \tag{7}$$

where S_n is the right shift map

$$S_n(\mathbf{x}) = (x_n, x_1, x_2, \dots, x_{n-1})$$

for $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{Z}_2^n$.

For odd n, let $\mathcal{C}_n$ be the subspace of $\mathbb{Z}_2^n$ consisting of all vectors $(x_1, x_2, \ldots, x_n)$ for which the number of 1's among $x_1, x_2, \ldots, x_n$ is even.

Now, for odd n, we can characterize all vectors that belong to a cycle.

Lemma 4.1 *Let $\mathbf{x} \in \mathbb{Z}_2^n$ for odd n. Then $\mathbf{x}$ is in a cycle for D_n if and only if it belongs to $\mathcal{C}_n$. Similarly, $\mathbf{x}$ is in a cycle for M_n if and only if it belongs to $\mathcal{C}_n$. Therefore, $\mathbf{x}$ is in a cycle for D_n if and only if it is in a cycle for M_n.*

Proof Assume that n is odd. If $\mathbf{x} \in \mathbb{Z}_2^n$ then $D_n(\mathbf{x})$ and $M_n(\mathbf{x})$ belong to $\mathcal{C}_n$ (this is clearly true for every vector from the natural basis of $\mathbb{Z}_2^n$, so since $\mathcal{C}_n$ is a linear subspace, it is true for every vector). On the other hand, if $\mathbf{y} \in \mathbb{Z}_2^n$ is given and we try to find its preimage $\mathbf{x}$ under D_n or M_n, we can do it in the unique way when we fix the first component of $\mathbf{x}$. Moreover, the two preimages we find in such a way have sum $(1, 1, \ldots, 1)$, so exactly one of them belongs to $\mathcal{C}_n$. This means that D_n and M_n are one-to-one on $\mathcal{C}_n$, and therefore each vector from $\mathcal{C}_n$ belongs to a cycle. $\square$

Applying Lemma 4.1, we will establish a formula relating the maximal cycle lengths of D_n and M_n. Before we state it, let us note that for an odd n the vectors with two adjacent 1's and 0's otherwise form a basis of $\mathcal{C}_n$. Clearly, they belong to cycles of the same length k of D_n. Therefore $D_n^k(\mathbf{x}) = \mathbf{x}$ for any $\mathbf{x} \in \mathcal{C}_n$. This means that k is the maximal cycle length for D_n and all cycle lengths for D_n divide k. Clearly, the same holds for M_n.

Theorem 4.2 *Let $c_{D,n}$ be the maximal cycle length for D_n and let $c_{M,n}$ be the maximal cycle length for M_n. Then $c_{D,n} = \mathrm{lcm}(n, c_{M,n})$.*

Proof Let n be odd. We will first show that the $\mathrm{lcm}(n, c_{M,n}) | c_{D_n}$. Let $D_{L,n} = I + T_n$ and $D_{R,n} = I + S_n$ where T_n is the left shift map and S_n is the right shift map on $\mathbb{Z}_2^n$. Observe that $D_{L,n} = D_n$ and $D_{L,n} D_{R,n} = M_n$. The maps $D_n, D_{L,n}$ and $D_{R,n}$ all commute and moreover, because $D_{L,n}$ and $D_{R,n}$ share the same minimal polynomial, the maximal cycle length of D_n equals the maximal cycle length of $D_{R,n}$. As stated at the end of Section 3, the image of any vector under D_n belongs to a cycle of D_n. As a result, $D_n^{c_{D,n}+1} = D_n$ and therefore,

$$M_n^{c_{D,n}+1} = D_{L,n}^{c_{D,n}+1} D_{R,n}^{c_{D,n}+1} = D_{L,n} D_{R,n} = M_n$$

and so $M_n^{c_{D,n}+1} - M_n = 0$. Because the minimal polynomial of $A_{M,n}$ divides any other polynomial that annihilates $A_{M,n}$, the minimal polynomial of $A_{M,n}$ divides $\lambda^{c_{D,n}+1} - \lambda$. From [18] we know that $\mu_{M,n}(\lambda) = \lambda \tilde{\mu}_{M,n}(\lambda)$ and as a result, $\tilde{\mu}_{M,n}(\lambda) | \lambda^{c_{D,n}} - 1$. Thus, the order of $\mu_{M,n}$ divides $c_{D,n}$. By Theorem 2.3 the order of $\mu_{M,n}$ equals $c_{M,n}$ proving that $c_{M,n} | c_{D,n}$. A result in [5] states that $n | c_{D,n}$ yielding $\mathrm{lcm}(n, c_{M,n}) | c_{D,n}$.

We will now prove that $c_{D,n} | c_{M,n}$. By Lemma 4.1 and the remark preceding the

statement of the theorem that we are proving, we know that on the subspace $\mathcal{C}$, $M_n^{c_{M,n}} = I$. Let $b = \text{lcm}(n, c_{M,n})$. Then on $\mathcal{C}$

$$(D_n^2)^b = D_n^{2b} = T_n^{2b} M_n^{2b} = I.$$

Thus, $c_{D,n}|2b$. In [5], $c_{D,n}$ was shown to be odd for odd n. Therefore, $c_{D,n}|b$.

Martin, Odlyzko and Wolfram proved in [13] if $n = 2^j r$ for r odd that $c_{M,n} = 2^j c_{W,r}$. This result and Corollary 3.2 imply

$$c_{D,n} = 2^j c_{D,r} = 2^j \text{lcm}(r, c_{w,r}) = \text{lcm}(n, c_{M,n}),$$

proving the result in the even case. □

The results in this section are algebraic and rely on the language of minimal annihilating polynomials. Unfortunately, this method of analysis is restricted to fields and consequently cannot be extended to ring modules. Both D_n and M_n share symmetry properties that can be viewed geometrically. A geometric approach is more likely to suggest how results can be extended to ring modules.

4.1 Geometry of the maps D_n and M_n.

In order to use the connection between D_n and M_n to relate the transient and cyclic behavior of both maps, we need more information than (7) provides. It is desirable to have a conjugacy relationship that directly identifies dynamics of one map to the other. For $n = 2k + 1$ and $x = (x_1, x_2, x_3, \ldots, x_{2k+1}) \in \mathbb{Z}_2^n$, the permutation that orders all terms of x with odd indices first and followed by all even indexed terms

$$\sigma(x) = (x_1, x_3, \ldots, x_{2k+1}, x_2, x_4, \ldots, x_{2k}),$$

satisfies

$$\sigma M_n \sigma^{-1} = D_n T_n^k.$$

As a result, for $n = 2k + 1$, M_n is conjugate to the map $V_n = D_n T_n^k$.

In order to view iteration geometrically, we think of the components of a vector in $\mathbb{Z}_2^n$ as states of vertices on a regular n-gon and examine the action of D_n or M_n on the vertices. For example, Figure 1 depicts successive iterations of M_5 on the initial vector $(1, 1, 0, 0, 0)$. Notice that the states are symmetric with respect to the dashed line drawn in each polygon. This line is called an *axis of symmetry* and each of these vectors is symmetric with respect to this axis.

Definition 4.3 *Let $n = 2k + 1$. Let $U_{n,i}$ be the the symmetry map about the i-th axis, that is $U_{n,i}(x_1, x_2, \ldots, x_n) = (x_{2i-1}, x_{2i-2}, \ldots, x_{2i-n})$. A vector* $\mathbf{x}$ *is*

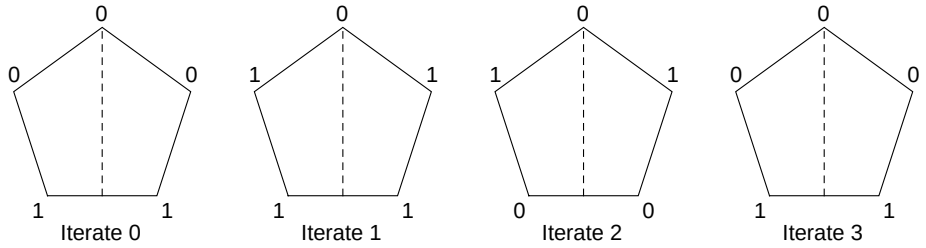

Fig. 1. Images of $b_1 = (1, 1, 0, 0, 0, 0)$ under iterates of M_5.

said to be symmetric with respect to the i-th axis, if $U_{n,i}(\mathbf{x}) = \mathbf{x}$ and $x_i = 0$. We say that a vector is symmetric if it is symmetric with respect to some axis.

We added in the definition an extra condition that $x_i = 0$ in order to assure that there is even number of 1's among $x_1, x_2, \ldots, x_n$, so that any symmetric vector belongs to $\mathcal{C}_n$.

Clearly, the set $\mathcal{S}_{n,i}$ of all vectors symmetric with respect to the i-th axis is a linear subspace.

Theorem 4.4 *The subspace $\mathcal{S}_{n,i}$ is invariant for V_n, that is, $V_n(\mathcal{S}_{n,i}) = \mathcal{S}_{n,i}$.*

Proof Since $D_n = I + T_n$, we get $V_n = T_n^k + T_n^{k+1} = T_n^k + S_n^k$. Clearly, $T_n U_{n,i} = U_{n,i} S_n$ and $S_n U_{n,i} = U_{n,i} T_n$. Therefore

$$U_{n,i} V_n = U_{n,i} T_n^k + U_{n,i} S_n^k = S_n^k U_{n,i} + T_n^k U_{n,i} = V_n U_{n,i}.$$

Therefore, if $\mathbf{x} \in \mathcal{S}_{n,i}$ then

$$U_{n,i}(V_n(\mathbf{x})) = V_n(U_{n,i}(\mathbf{x})) = V_n(\mathbf{x}).$$

Moreover, $V_n(\mathbf{x}) = D_n(T_n^k(\mathbf{x})) \in \mathcal{C}_n$. Those two properties together imply that $V_n(\mathbf{x}) \in \mathcal{S}_{n,i}$.

On the other hand, since $\mathcal{S}_{n,i} \subset \mathcal{C}_n$, the map V_n is one-to-one there, so we get $V_n(\mathcal{S}_{n,i}) = \mathcal{S}_{n,i}$. $\square$

The symmetry property held by V_n yields a geometrical proof of Theorem 4.2.

An alternate proof of Theorem 4.2. We need prove the result only for n odd because the even case follows immediately as in the proof of Theorem 4.2.

As we noticed in the paragraph preceding the statement of Theorem 4.2 (cf. [18]), the vector $\mathbf{b}_1 = V_n(\mathbf{e}_1)$ belongs to a maximal cycle under M_n.

Let d be the smallest nonnegative integer such that

$$V_n^d(\mathbf{b}_1) = S_n^m(\mathbf{b}_1)$$

for some nonnegative integer m. Clearly, $\mathbf{b}_1 \in \mathcal{S}_{n,i}$, so by Theorem 4.4 also $V_n^d(\mathbf{b}_1) \in \mathcal{S}_{n,i}$. The only power of the right shift applied to $\mathbf{b}_1$ that results in a vector symmetric with respect to the first axis is the zeroth one. Therefore,

$$V_n^d(\mathbf{b}_1) = \mathbf{b}_1,$$

and consequently $c_{M,n}|d$.

Now suppose there exists a vector $\mathbf{u}$ such that $V^{c_{M,n}}(\mathbf{u}) = \mathbf{u}$. By definition of V_n, $D_n^{c_{M,n}}(\mathbf{u}) = T_n^k(\mathbf{u})$, which implies $d|c_{M,n}$. Therefore, $c_{M,n} = d$.

Now d is the maximal period of D_n modulo shifts. As a result, $c_{D,n} = \text{lcm}(n, d)$ $= \text{lcm}(n, c_{M,n})$. $\square$

Both arguments for Theorem 4.2 rely on the fact that n is odd. However, Corollary 3.2 and the end of the first proof of Theorem 4.2 indicate that there is a reduction from dimension $2n$ to dimension n. Table 1 suggests that the reduction may hold true for all cycle lengths, not just the maximal ones. For example when $n = 6$ the cycle lengths of M_n are $1, 2$. The cycle lengths for $n = 12$ are $1, 2, 4$. It seems that the cycle lengths for $n = 6$ reappear as cycle lengths for $n = 12$ with the addition of a new cycle length of 4 which was merely double an old cycle length.

Motivated by the data, we investigate how to identify periodic vectors in dimension n with periodic vectors in dimension $2n$.

5 Cyclic dynamics for dimension $2n$

We are interested in using the dynamics of a map in dimension n to arrive at the dynamics of the map extended to dimension $2n$. The motivation for this goal is illustrated using D_n. Similar computations can be performed for M_n.

Let $g_1, g_2 : \mathbb{Z}_2^n \to \mathbb{Z}_2^{2n}$ be the linear embeddings defined by

$$g_1(\mathbf{x}) = (0, x_1, 0, x_2, \ldots, 0, x_n) \tag{8}$$
$$g_2(\mathbf{x}) = (x_1, 0, x_2, 0, \ldots, x_n, 0) \tag{9}$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$. Direct computation yields

$$D_{2n}(g_1(\mathbf{x})) = g_1(\mathbf{x}) + g_2(\mathbf{x}) \tag{10}$$

and

$$D_{2n}(g_2(\mathbf{x})) = g_1(T_n(\mathbf{x})) + g_2(\mathbf{x}). \tag{11}$$

Using (10) and (11) along with $D_n = I + T_n$ gives

$$\begin{aligned} D_{2n}^2(g_1(\mathbf{x})) &= g_1(D_n(\mathbf{x})), \\ D_{2n}^2(g_2(\mathbf{x})) &= g_2(D_n(\mathbf{x})), \end{aligned}$$

which in Cartesian product form is

$$D_{2n}^2(g_1(\mathbf{x}_1), g_2(\mathbf{x}_2)) = (g_1(D_n(\mathbf{x}_1)), g_2(D_n(\mathbf{x}_2)). \tag{12}$$

Let $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}_2^n$ belong to cycles of length k_1 and k_2 respectively. Let $k = \text{lcm}(k_1, k_2)$ and $\mathbf{y} = (g_1(\mathbf{x}_1), g_2(\mathbf{x}_2))$. Then repeated applications of (12) together with the periodicity of $\mathbf{x}_i, i = 1, 2$, give

$$D_{2n}^{2k}(\mathbf{y}) = (g_1(D_n^k(\mathbf{x}_1)), g_2(D_n^k(\mathbf{x}_2))) = (g_1(\mathbf{x}_1), g_2(\mathbf{x}_2)) = \mathbf{y}. \tag{13}$$

Thus, $\mathbf{y}$ belongs to a cycle under D_{2n}. Let m be the length of that cycle. Clearly, $m|2k$ by (13).

In addition, (12) and the periodicity of $\mathbf{y}$ yield

$$(g_1(\mathbf{x}_1), g_2(\mathbf{x}_2)) = D_{2n}^{2m}((g_1(\mathbf{x}_1), g_2(\mathbf{x}_2)) = (g_1(D_n^m(\mathbf{x}_1)), g_2(D_n^m(\mathbf{x}_2))).$$

Hence, $D_n^m(\mathbf{x}_i) = \mathbf{x}_i$ for $i = 1, 2$, resulting in $k|m$. Consequently, $m = k$ or $2k$.

If we know further that $m = 2j$ for some nonnegative integer j, then

$$D_{2n}^{2j}((g_1(\mathbf{x}_1), g_2(\mathbf{x}_2)) = (g_1(D_n^j(\mathbf{x}_1)), g_2(D_n^j(\mathbf{x}_2))),$$

which again by periodicity equals $\mathbf{y}$. As before, $D_n^j(\mathbf{x}_i) = \mathbf{x}_i$ for $i = 1, 2$, which implies $k|j$. Therefore, in this case, $m = 2k$.

The conclusions relating cycle lengths require only the condition expressed in (12) and, therefore, we can state the following generalization.

Theorem 5.1 *Let X_1, X_2 be any two sets and consider maps $G_i : X_i \to X_i$, $i = 1, 2$. For $i = 1, 2$ suppose that X_i is embedded in Y_i by the injections g_i. Assume further that $Y = Y_1 \times Y_2$ and F is a map from Y into Y satisfying,*

$$F^2(g_1(\mathbf{x_1}), g_2(\mathbf{x_2})) = (g_1(G_1(\mathbf{x_1})), g_2(G_2(\mathbf{x_2}))). \tag{14}$$

If $\mathbf{x_i}$ is in a cycle of length k_i under G_i for $i = 1, 2$, with $k = \text{lcm}(k_1, k_2)$, then

(1) The point $\mathbf{y} = (g_1(\mathbf{x_1}), g_2(\mathbf{x_2}))$ belongs to a cycle of some length m.
(2) Either $m = k$ or $m = 2k$.

(3) If m is even, then $m = 2k$.

The calculations in the previous example did not require $G_1 = G_2$ or $X_1 = X_2$ and therefore, the proof of the theorem proceeds by the same computations (generalized) in the example with $X_i = \mathbb{Z}_2^n$, $G_i = D_n$, $Y_i = g_i(X_i)$ for $i = 1, 2$ and $F = D_{2n}$. Consequently, the proof will be omitted.

It is desirable to find out when k equals m and when $2m$. In order to achieve this goal more structural knowledge of the maps and the sets is required. Once again, we motivate the idea using D_n.

Example Assume the notation of the Ducci example. In this example we will show that in the case $k = 2j + 1$ for some nonnegative integer j, we have $k = m$ if and only if

$$\mathbf{x}_1 = D_n^j(\mathbf{x}_1) + T_n D_n^j(\mathbf{x}_2), \tag{15}$$
$$\mathbf{x}_2 = D_n^j(\mathbf{x}_1) + D_n^j(\mathbf{x}_2).. \tag{16}$$

Using (12) and the linearity of D_{2n} yields

$$\begin{aligned} D_{2n}^k(\mathbf{y}) &= D_{2n}(D_{2n}^{2j}(\mathbf{y})) = D_{2n}(g_1(D_n^j(\mathbf{x}_1)) + g_2(D_n^j(\mathbf{x}_2)) \\ &= D_{2n}(g_1(D_n^j(\mathbf{x}_1))) + D_{2n}(g_2(D_n^j(\mathbf{x}_2))) \end{aligned}$$

Properties (10) and (11) and the linearity of the isomorphisms result in

$$\begin{aligned} & D_{2n}(g_1(D_n^j(\mathbf{x}_1))) + D_{2n}(g_2(D_n^j(\mathbf{x}_2))) \\ &= g_1(D_n^j(\mathbf{x}_1)) + g_2(D_n^j(\mathbf{x}_1)) + g_1(T_n(D_n^j(\mathbf{x}_2))) + g_2(D_n^j(\mathbf{x}_2)) \\ &= g_1(D_n^j(\mathbf{x}_1) + T_n(D_n^j(\mathbf{x}_2))) + g_2(D_n^j(\mathbf{x}_1) + D_n^j(\mathbf{x}_2)). \end{aligned} \tag{17}$$

Assume that $k = m$. Then by periodicity, $D_{2n}^k(\mathbf{y}) = \mathbf{y}$, and so the final right-hand side in (17) is equal to $g_1(\mathbf{x}_1) + g_2(\mathbf{x}_2)$. Because g_1 and g_2 are one-to-one, equating arguments yields (15) and (16).

On the other hand, assuming (15) and (16) and applying the conditions to (17) results in $D_{2n}^k(\mathbf{y}) = \mathbf{y}$. Therefore, $m|k$, so by Theorem 5.1 (2), we have $m = k$.

As usual, similar computations can be performed for M_n. Generalizing these examples, we arrive at the following corollary.

Corollary 5.2 *Suppose that in Theorem 5.1 $X = X_1 = X_2$ is a vector space and assume that F, g_1 and g_2 are linear and that $G = G_1 = G_2$. Assume*

further that there exist maps A_i, B_i for $i = 1, 2$ such that

$$F(g_1(\mathbf{z})) = g_1(A_1(\mathbf{z})) + g_2(A_2(\mathbf{z})) \tag{18}$$

and

$$F(g_2(\mathbf{z})) = g_1(B_1(\mathbf{z})) + g_2(B_2(\mathbf{z})) \tag{19}$$

for all $\mathbf{z} \in X$. Then, when $k = 2j+1$ for some nonnegative integer j, we have $m = k$ if and only if

$$\mathbf{x_1} = A_1(G^j(\mathbf{x}_1)) + B_1(G^j(\mathbf{x}_2)) \tag{20}$$

and

$$\mathbf{x_2} = A_2(G^j(\mathbf{x}_1)) + B_2(G^j(\mathbf{x}_2)). \tag{21}$$

Proof Applying (14), the linearity of F and then (18) and (19) yields

$$\begin{aligned}
&F^k(g_1(\mathbf{x}_1) + g_2(\mathbf{x}_2)) = F(F^{2j}(g_1(\mathbf{x}_1) + g_2(\mathbf{x}_2))) \\
&= F(g_1(G^j(\mathbf{x}_1)) + g_2(G^j(\mathbf{x}_2))) \\
&= F(g_1(G^j(\mathbf{x}_1))) + F(g_2(G^j(\mathbf{x}_2))) \\
&= g_1(A_1(G^j(\mathbf{x}_1))) + g_2(A_2(G^j(\mathbf{x}_1))) + g_1(B_1(G^j(\mathbf{x}_2))) + g_2(B_2(G^j(\mathbf{x}_2))) \\
&= g_1(A_1(G^j(\mathbf{x}_1)) + B_1(G^j(\mathbf{x}_2))) + g_2(A_2(G^j(\mathbf{x}_1)) + B_2(G^j(\mathbf{x}_2))).
\end{aligned} \tag{22}$$

If $k = m$, then periodicity of F leads to $g_i(A_i(G^j(\mathbf{x}_1)) + B_i(G^j(\mathbf{x}_2))) = g_i(\mathbf{x}_i)$ for $i = 1, 2$. Equating arguments we arrive at (20) and (21).

On the other hand, if (20) and (21) hold, then applying the conditions to (22) implies $F^k(\mathbf{y}) = \mathbf{y}$. As a result, $m|k$ so by Theorem 5.1 we get $m = k$. □

For the case of the Ducci map, $A_1 = I$, $A_2 = I$, $B_1 = T_n$ and $B_2 = I$. For the MOW map, $A_1 = 0$, $A_2 = I + S_n$, $B_1 = I + T_n$ and $B_2 = 0$. In both cases, A_2 and B_1 are invertible on $\mathcal{C}_n$, which allows us to solve the system (20) and (21):

$$\mathbf{x_1} = A_1A_2^{-1}(\mathbf{x}_2) + B_1(G^j(\mathbf{x}_2)) + A_1A_2^{-1}B_2(G^j(\mathbf{x}_2)), \tag{23}$$

$$\mathbf{x_2} = B_2B_1^{-1}(\mathbf{x}_1) + A_2(G^j(\mathbf{x}_1)) + B_2B_1^{-1}A_1(G^j(\mathbf{x}_1)). \tag{24}$$

Therefore, when A_2 and B_1 are invertible, $\mathbf{x_1}$ is a function of $\mathbf{x_2}$ and vice versa. In this case, we can count the number of periodic vectors in dimension $2n$ as a function of the number of periodic vectors in dimension n.

Corollary 5.3 *Let X, F, G, A_i and B_i be defined as in Corollary 5.2. Assume further that A_2 and B_1 are invertible and that G commutes with A_i and B_i for $i = 1, 2$. Then for $k = 2j + 1$, $k = m$ implies $k_1 = k_2$.*

Proof Assume that $k = m$. Because A_2 and B_1 are invertible, conditions (23) and (24) hold. Applying (23), the commuting property of G and periodicity of $\mathbf{x_2}$ yields,

$$\begin{aligned} G^{k_2}(\mathbf{x}_1) &= A_1 A_2^{-1}(G^{k_2}(\mathbf{x}_2)) + B_1(G^j(G^{k_2}(\mathbf{x}_2))) + A_1 A_2^{-1} B_2(G^j(G^{k_2}(\mathbf{x}_2))) \\ &= A_1 A_2^{-1}(\mathbf{x}_2) + B_1(G^j(\mathbf{x}_2)) + A_1 A_2^{-1} B_2(G^j(\mathbf{x}_2)) = \mathbf{x_1}. \end{aligned}$$

As a result, $k_1 | k_2$. Similarly, applying Condition (24) shows $k_2 | k_1$. Thus, $k_1 = k_2$. □

One can easily check that D_n and M_n satisfy the assumptions of Corollary 5.3.

If X is finite dimensional of dimension n, Theorem 5.1 and Corollaries 5.2 and 5.3 provide us with a method to count the number of periodic vectors in dimension $2n$. To this end denote by $P(n, q)$ the number of vectors in dimension n belonging to a cycle of length q. The next theorem states several combinatorial results.

Theorem 5.4 *Suppose that the assumptions of Corollary 5.2 are satisfied and assume that X has dimension n. Then*

(1) If m is odd and the assumptions of Corollary 5.3 are satisfied, then
$P(2n, m)$
$= P(n, m)$.
(2) If m is even and k is odd, then $P(2n, 2k) = \sum P(n, k_1)P(n, k_2) - P(n, k)$, where the sum is taken over all possible pairs (k_1, k_2) such that $k = \mathrm{lcm}(k_1, k_2)$.
(3) If m is even and k is even, then $P(2n, 2k) = \sum P(n, k_1)P(n, k_2)$, where the sum is taken over all possible pairs (k_1, k_2) such that $k = \mathrm{lcm}(k_1, k_2)$.

Proof Let us use the notation of Theorem 5.1 and Corollaries 5.2 and 5.3. Assume first that m is odd. By Theorem 5.1 (2), we have $m = k$. If the assumptions of Corollary 5.3 are satisfied, we get $m = k = k_1 = k_2$. Since (24) represents the unique solution (for $\mathbf{x}_2$ in terms of $\mathbf{x}_1$) of the system (20) and (21), by Corollary 5.2 we get a one-to-one correspondence between the vectors $\mathbf{x}_1$ from X belonging to a cycle of length m and the vectors $\mathbf{y}$ from Y belonging to a cycle of length m. This proves (1).

Assume now that m is even. By Theorem 5.1 (3), we have $m = 2k$. Thus, the vectors $\mathbf{y}$ counted in $P(2n, m)$ are exactly these for which $\mathbf{x}_1$ is counted in $P(n, k_1)$, $\mathbf{x}_2$ is counted in $P(n, k_2)$ and $k = \mathrm{lcm}(k_1, k_2)$, except the vectors that we considered in the preceding paragraph (because those vectors $\mathbf{y}$ belong to cycles of length $k = m/2$; this of course affects only the case of k odd). This proves 2 and 3. □

We illustrate how to apply Theorem 5.4 for $n = 3, 6$ and 12 using the Ducci map.

Example Under D_n with $n = 3$ there is one fixed vector and there are three vectors of period 3.

Vector	**Cycle length**
$(0,0,0)$	1
$(0,1,1)$	3
$(1,0,1)$	3
$(1,1,0)$	3

Table 2
Cyclic vectors for $n = 3$ with corresponding cycle length.

By Theorem 5.1, $n = 6$ has possible periods of $1, 2, 3$ and 6. To count the number of vectors that belong to a cycle where the length m is odd we apply (1) of Theorem 5.4.

$$P(6,1) = P(3,1) = 1,$$
$$P(6,3) = P(3,3) = 3.$$

The only possible cases with m even are $m = 2$ and $m = 6$. The vectors $\mathbf{x_1} = (0,0,0)$ and $\mathbf{x_2} = (0,0,0)$ would yield the only candidate for a period 2 vector in dimension six. However, $(0,0,0,0,0,0)$ has period 1 and hence there are no period 2 vectors for $n = 6$. This fact can be also arrived at applying (2). The only possible pair $k_1 = 1, k_2 = 1$ gives $P(3,1) = 1$. Subtracting $P(3,1) = 1$ from the product results in a total of 0 vectors of period 2.

For $m = 6$, $k = 3$ we can see that all possible pairs such that $3 = \text{lcm}(k_1, k_2)$ are $(1,3), (3,1)$ and $(3,3)$. Applying (2) gives,

$$\begin{aligned} P(6,6) &= P(3,1)P(3,3) + P(3,3)P(3,1) + P(3,3)P(3,3) - P(3,3) \\ &= 1 \cdot 3 + 3 \cdot 1 + 3 \cdot 3 - 3 = 15 - 3 = 12. \end{aligned}$$

Using $\mathbf{y} = g_1(\mathbf{x}_1) + g_2(\mathbf{x}_2)$, each periodic vector $\mathbf{y} \in \mathbb{Z}_2^6$ can be constructed along with corresponding period.

Just as the information was lifted from dimension 3 to dimension 6 we now use the $n = 6$ data to count the cyclic vectors in dimension 12. Applying Theorem 5.4 yields

Vector	Cycle length	Vector	Cycle length
$(0,0,0,0,0,0)$	1	$(0,0,1,1,1,1)$	6
$(0,1,1,0,1,1)$	3	$(1,0,0,1,1,1)$	6
$(1,0,1,1,0,1)$	3	$(0,1,0,0,0,1)$	6
$(1,1,0,1,1,0)$	3	$(1,1,1,1,0,0)$	6
$(0,0,1,0,1,0)$	6	$(1,1,0,0,1,1)$	6
$(1,0,0,0,1,0)$	6	$(1,1,1,0,0,1)$	6
$(1,0,1,0,0,0)$	6	$(0,1,0,1,0,0)$	6
$(0,0,0,1,0,1)$	6	$(0,1,1,1,1,0)$	6

Table 3
Cyclic vectors for $n = 6$ with corresponding cycle length.

$$
\begin{aligned}
P(12,1) &= P(6,1) = 1 \quad (m \text{ odd}),\\
P(12,3) &= P(6,3) = 3 \quad (m \text{ odd}),\\
P(12,2) &= P(6,1)P(6,1) - P(6,1) = 0 \quad (m \text{ even},\ k \text{ odd}),\\
P(12,6) &= P(6,3)P(6,1) + P(6,1)P(6,3) + P(6,3)P(6,3) - P(6,3)\\
&= 12 \ (m \text{ even},\ k \text{ odd}),\\
P(12,12) &= P(6,1)P(6,6) + P(6,6)P(6,1) + P(6,3)P(6,6)\\
&\quad + P(6,6)P(6,3) + P(6,6)P(6,6) = 240 \quad (m \text{ even},\ k \text{ even}).
\end{aligned}
$$

References

[1] F. Breuer, F., Lőtter and B. van der Merwe, Ducci sequences and cyclotomic polynomials, preprint.

[2] N. Calkin, J. Stevens and D. Thomas, A characterization of lengths of cycles of the n-number Ducci game, Fibonacci Quarterly, in press.

[3] M. Chamberland, Unbounded Ducci sequences, J. Difference Equ. Appl., 2003, 9, 887-895.

[4] M. Chamberland and D. Thomas, The n-number ducci game (open problems and conjectures), J. Difference Equ. Appl., 2004, 10, 339-342.

[5] A. Ehrlich, Periods in Ducci's n-number game of differences, Fibonacci Quart., 1990, 28, 302-305.

[6] H. Glaser and G. Schöffl, Ducci-sequences and Pascal's triangle, Fibonacci Quart., 1995, 33, 313-324.

[7] R. Honsberger, *Ingenuity in mathematics*,1970, Yale University.

[8] N. Jacobson, *Lectures in abstract algebra. Vol. II. Linear Algebra*, 1953, Van Nostrand Co., Toronto-New York-London.

[9] E. Jen, Cylindrical cellular automata, Comm. Math. Phys., 1988, 118, 569-590.

[10] E. Jen, Linear cellular automata and recurring sequences in finite fields, Comm. Math. Phys., 1988, 119, 13-28.

[11] R. Lidl and H. Niederreiter, *Finite fields, Encyclopedia of Mathematics and its Applications*, 1983, 20, Addison-Wesley, Reading, MA.

[12] A. Ludington Furno, Cycles of differences of integers, J. Number Theory, 1981, 13, 255-261.

[13] O. Martin, A. Odlyzko and S. Wolfram, Algebraic properties of cellular automata, Comm. Math. Phys., 1984, 93, 219-258.

[14] J. C. P. Miller, Periodic forests of stunted trees, Philos. Trans. Roy. Soc. Lond., 1970, A266, 63-111.

[15] M. Misiurewicz and A. Schinzel, On n numbers on a circle, Hardy-Ramanujan Journal, 1988, 11, 30-39.

[16] J. Stevens, R. Rosensweig and A. Cerkanowicz, Transient and cyclic behavior of cellular automata with null boundary Conditions, J. Statist. Phys., 1993, 73, 159-174.

[17] J. G. Stevens, On the construction of state diagrams for cellular automata with additive rules, Inform. Sci., 1999, 115, 43-59.

[18] S. Lettieri, J. G. Stevens and D. M. Thomas, Characteristic and minimal polynomials of linear cellular automata, Rocky Mountain J. Math. (in press).

[19] F. Vivaldi, Geometry of linear maps over Finite Fields, Nonlinearity , 5, (1992), 133-147.

[20] S. Wolfram, *A new kind of science*, 2002, Wolfram Media, Champaign, IL.